UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/518,664 | 03/03/2000 | Cameron Mashayekhi | 112024-0054 | 6178 |

21186 7590 01/04/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH
1600 TCF TOWER
121 SOUTH EIGHT STREET
MINNEAPOLIS, MN 55402

| EXAMINER | |
|---|---|
| HENEGHAN, MATTHEW E | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

DATE MAILED: 01/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/518,664 | MASHAYEKHI, CAMERON | |
| | Examiner | Art Unit | |
| | Matthew Heneghan | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *19 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 19 September 2005 has been entered.

2. In response to the most recent office action, claims 1, 9, and 15 have been amended. Claims 1-20 have been examined.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-11, 13, 15, 17, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,401,206 to Khan et al. in view of U.S. Patent No. 5,818,936 to Mashayekhi further in view of Menezes, "Handbook of Applied Cryptography," 1997, pp. 494, 515, and 516.

Regarding claims 1, 3, 4, 7-11, 13, 15, 17, 18, and 20, the system disclosed by Khan, a local interface receives private user information and stored user secrets, which are used to generate authentication secrets (see column 6, lines 37-58). A session key is created (see column 7, lines 1-4). Khan employs prior art encryption procedures, including a symmetric key algorithm (column 5, lines 36-40), which generates the common key. The common key is then encrypted using a public key (the "session key", which, being public, is inherently transmitted) for transmission (see column 5, lines 43-48). Employing this system, an authentication database takes the entered secrets and encrypts them using the common key (see column 8, lines 30-36). The encrypted secret, the encrypted common key, and the session key are therefore transmitted to the receiver. Since a symmetric key is used for the common key, it is a shared and same key for both ends of the transmission.

Khan further discloses that this technique can be used for any application where a user's identity needs to be verified, such as logging on to computers (see column 12, line 66 to column 13, line 50). Khan does not explicitly mention the accessing of network resources, however.

Mashayekhi discloses a system for accessing network resources, wherein a user at a local workstation is authenticated using a network database contain several

program-specific user secrets, each having an identifier, a user-specific secret (see column 5, line 57 to column 6, line 30), and a network policy associated with the user in the form of an ACL (see column 6, lines 44-59). Mashayekhi further suggests that this strategy provides a means for easily and efficiently authenticating a user to various applications on a network (see column 3, lines 14-21).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement the method of Khan in a network resource accessing system, as disclosed by Mashayekhi, as this strategy provides a means for easily and efficiently authenticating a user to various applications on a network.

Khan also discloses the use of a public key method for key exchanging, but does not disclose that it is a session key.

Menezes discloses the Diffie-Hellman (a public key algorithm) key exchange algorithm for creating shared secrets (see Protocol 12.47) and further notes that such shared secrets constitute session keys (see p. 494, first 4 lines), and further notes that by the key may last the length of a single telecommunications session (i.e. established at logon, discarded at the end of the session). Menezes further suggests that such keys are used, for example, to limit exposure to key compromise (see Motivation for use of session keys, items 1-4).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further implement the method of Khan and

Mashyekhi by using the system in an using Diffie-Hellman derived keys as session keys, as disclosed by Menezes, to limit exposure to key compromise.

As per claims 2, 5, and 6, the algorithm is the symmetric key algorithm, and the key has been derived from secret, such as a PIN (see column 8, lines 30-36).

4. Claims 12, 14, 16, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,401,206 to Khan et al. in view of U.S. Patent No. 5,818,936 to Mashayekhi further in view of Menezes, "Handbook of Applied Cryptography," 1997, pp. 494, 515, and 516 as applied to claims 9 and 15 above, and further in view of U.S. Patent 5,869,565 to Spies et al.

Khan, Mashayekhi, and Menezes do not disclose the negotiating of an encryption algorithm.

Spies discloses an algorithm selection algorithm wherein the client sends a certificate indicative of its supported algorithms (thus containing a list of at least one algorithm) which the server compares with its table of available algorithms, from which it chooses the strongest. Spies further states that this may be necessary for regulatory compliance (see column 15, lines 10-44).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Khan and Mashayekhi to include the algorithm negotiation disclosed by Spies, as this may be necessary for regulatory compliance.

## *Response to Arguments*

5. Applicant's arguments with respect to claims 1, 9, and 15 have been considered but are moot in view of the new grounds of rejection.

The incorporation of Howard into the previous grounds of rejection was based upon its use of session keys, which could equally be applied to initial key establishment or rekeying. In the Request for Reconsideration filed 17 August 2005, Applicant argued that Howard could not be relied upon because it only taught to a re-keying process. In the subsequent Advisory Action mailed 2 September 2005, it was noted that, even if Howard's use of session keys only could be applied to a re-keying functionality, the claims as then written didn't preclude such a functionality.

Howard has been replaced by Menezes, above, in order to further establish the use of session keys in cryptographic systems for initial key establishment.

## *Conclusion*

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
**Or faxed to:**
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

December 15, 2005

David Y. Jung
Primary Examiner

12/23/05